KEARNEY& COMPANY

Certified Public Accountants and Consultants

4501 Ford Avenue, Suite 1400, Alexandria, VA 22302
PH: 703.931.5600, FX: 703.931.3655, www.kearneyco.com

Independent Auditor's Report on Internal Control

To the Architect of the Capitol

We have audited the financial statements of the Architect of the Capitol (AOC) as of and for the year ended September 30, 2007, and have issued our report dated January 16, 2008. We conducted our audit in accordance with auditing standards generally accepted in the United States of America, the standards applicable to financial audits contained in *Government Auditing Standards,* issued by the Comptroller General of the United States, and Office of Management and Budget (OMB) Bulletin No. 07-04, *Audit Requirements for Federal Financial Statements.* The management of AOC is responsible for maintaining effective internal control over financial reporting.

In planning and performing our audit, we considered AOC's internal control over financial reporting by obtaining an understanding of the design effectiveness of AOC's internal control, determining whether these controls had been placed in operation, assessing control risk, and performing tests of AOC's controls in order to determine our auditing procedures for the purpose of expressing our opinion on the financial statements and not to provide an opinion on the internal controls. Accordingly, we do not express an opinion on the effectiveness of AOC's internal control over financial reporting.

We limited our control testing to those controls necessary to achieve the following OMB control objectives that provide reasonable, but not absolute assurance, that: (1) transactions are properly recorded, processed, and summarized to permit the preparation of the financial statements in accordance with accounting principles generally accepted in the United States of America, and assets are safeguarded against loss from unauthorized acquisition, use, or disposition; (2) transactions are executed in compliance with laws governing the use of budget authority, government-wide policies and laws identified in Appendix E of OMB Bulletin No. 07-04, and other laws and regulations that could have a direct and material effect on the financial statements; and (3) transactions and other data that support reported performance measures are properly recorded, processed, and summarized to permit the preparation of performance information in accordance with criteria stated by management. We did not test all internal controls relevant to the operating objectives broadly defined by the Federal Managers' Financial Integrity Act of 1982.

A control deficiency exists when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent or detect misstatements on a timely basis. A significant deficiency is a control deficiency, or combination

of control deficiencies, that adversely affects AOC's ability to initiate, authorize, record, process, or report financial data reliably in accordance with generally accepted accounting principles such that there is more than a remote likelihood that a misstatement of AOC's financial statements that is more than inconsequential will not be prevented or detected by AOC's internal control.

A material weakness is a significant deficiency, or combination of significant deficiencies, that results in more than a remote likelihood that a material misstatement of the financial statements will not be prevented or detected by AOC's internal control. Our consideration of internal control was for the limited purpose described in the second paragraph of this report and would not necessarily identify all deficiencies in internal control that might be significant deficiencies or material weaknesses. We noted three matters, discussed below, involving the internal control and its operation that we consider to be material weaknesses.

MATERIAL WEAKNESSES

1. Internal Control Assessments (Repeat Condition)

AOC has not completed a formal and systematic assessment and evaluation of the design and operation of internal controls. As of September 30, 2007, AOC has completed an assessment of the procure to pay process, and has partially completed the human resource, time and attendance, and project management processes. In the absence of a complete assessment, AOC cannot determine if its current internal control design mitigates existing risks and effectively safeguards assets.

Recommendation – We recommend that AOC complete and document internal control assessments that evaluate the effectiveness of the design and operation of its internal control structure, including the identification of risks to material accounts and the existence of internal controls to mitigate those risks. Although AOC is not subject to OMB Circular A-123, *Management's Responsibility for Internal Control*, we recommend that AOC consult the "Implementation Guide for OMB Circular A-123, Appendix A, Internal Control over Financial Reporting" (the Guide). The Guide was issued by the Chief Financial Officer's Council in May 2005. The Guide includes guidance to enable management to evaluate internal controls and monitor and test these controls throughout the year.

2. Risk Assessment Updates (Repeat Condition)

The AOC internal control environment does not have a formal, documented process to monitor the internal and external environment, identify changing risk profiles, or respond accordingly. Specifically, AOC did not implement additional controls to reconcile the payroll data transmitted to and received from the National Finance Center (NFC), as recommended by NFC as an appendix to its qualified SAS 70 opinion. While several employees performed additional tests in response to the event, the actions were predicated on individual efforts, as compared to a repeatable and sustainable systemic effort.

Recommendation – We recommend that AOC develop a component in the internal control structure to monitor and identify changing risks. Also, AOC should reconcile NFC payroll data transmission to data receipt including, at a minimum, jurisdictional employees and hours.

3. Internal Control Design and Management of the Purchase to Disbursement Process (Modified Repeat Condition)

No organization/entity within AOC is accountable for the collective purchase to disbursement process. AOC has decentralized many components of the purchase and disbursement process, including initiating and coding requisitions, purchase authorizations, receiving, and disbursement approvals. Within a decentralized process, this lack of central monitoring and oversight results in a weakened control environment. This lack of internal control oversight and financial information integration includes the following:

- Seven individuals from two divisions had access and the ability to modify the vendor database with no process to ensure the propriety and accuracy of changes. In addition, supervisors did not approve vendor requests before new vendors were created in the system. Changes and modifications to the vendor database directly affect those to whom AOC can disburse funds.

- The jurisdictions' purchasing agents enter Budget Object Codes (BOCs) into purchase requisitions. However, the purchasing agents have received no financial training and have no written guidance to ensure consistent coding of transactions. Subsequent financial reporting and analyses is predicated upon the original coding. Additionally, AOC cannot readily search the financial records for certain transaction types, such as leases.

- AOC does not have a formal process to regularly review Construction Work in Progress projects with Project Managers after the project is initially established to ensure that accounting treatment is consistent with actual project activity. We identified one project, which contained a component that did not qualify for capitalization. We also questioned the proper capitalization of approximately ten other projects. While AOC was later able to justify the capitalization, AOC conducted the research in response to our queries, instead of as an integral component of the financial statement preparation process.

Recommendation – We recommend that AOC assign formal authority for oversight and monitoring of the process, including risk assessments and control design. This assessment should focus on interchange points between all process participants to ensure that financial statement risks are adequately mitigated. We also recommend limiting access to the vendor database to a select number of individuals, and that proposed changes be reviewed and approved before data entry. Data entry should also be reviewed for accuracy by a bipartisan, third party.

SIGNIFICANT DEFICIENCIES

1. Information System Controls (Repeat Condition)

We evaluated AOC's information system general controls following guidance provided by the National Institute of Standards and Technology (NIST) and the Government Accountability Office's (GAO) Federal Information System Controls Audit Manual (FISCAM). We provided a detailed report, as well as a prioritization of findings, under separate cover. For detailed descriptions of and recommendations for these findings, refer to the separately issued report.

We continue to identify areas for improvement in the implementation of AOC's security program as a result of the absence of key security personnel, such as the Chief Information Security Officer (CISO). However, AOC's incumbent CISO has made progress in improving its overall security program over the past few months. Progress includes the following:

- Initiating a plan for improvement; actions currently in progress include:
  - Identification of threats, analysis of impacts, determination of risks, recommendation of controls
  - Reviews of past risk assessment results, certification and accreditation (C&A) documentation, and third-party control assessments (SAS 70)
- Revising AOC's Information Security Program Policy and related procedures
- Improving controls over the modification of application software
- Developing an Interconnection Security Agreement with third-party service providers
- Initiating a Security Awareness Training plan
- Developing a C&A completion action plan and timeline.

While these efforts are important to reducing risk associated with identified deficiencies, they do not substantially change the information technology (IT) control environment.

Having noted improvements, AOC still has areas of weakness that need to be addressed. Some of the salient findings from that report appear below. Findings are reported under the following general categories:

- Entity-wide Security Program (SP)
- Access Control (AC)
- Service Continuity (SC).

Entity-wide Security Program

This category provides a framework and continuing cycle of activity for managing risk, developing security policies, assigning responsibilities, and monitoring the adequacy of the entity's computer-related controls. We noted weaknesses in the following areas relating to AOC's entity-wide SP:

- Risk assessments for financial and core operational components
- Information Systems Security Plans (ISSP) are not fully implemented
- Incident response procedures
- Detailed hiring procedures
- Security awareness and technical security training
- Effectiveness of corrective action process.

Access Control

Controls within this category limit or detect access to computer resources (i.e., data, programs, equipment, and facilities), thereby protecting these resources against unauthorized modification, loss, and disclosure. We noted weaknesses in the following areas relating to the AOC's AC:

- Defining and documenting user profiles
- De-provisioning and reassessing user accounts and assigned privileges
- Administration of special access privileges and the control of emergency and temporary authorizations
- Implementing tools and formalizing procedures for the handling of security violations.

Service Continuity

The controls in this category prevent loss of the capability to process, retrieve, and protect information maintained electronically. In prior years, we noted weaknesses related to the comprehensive Continuity of Operations Plan (COOP) and/or Disaster Recovery Plan (DRP). For the current year, we noted that AOC made improvements in this area by developing procedures for restoring IT services, backing up data, and performing testing of failover procedures. However, AOC needs to define continuity planning for major applications to ensure business-related activities can resume in a timely manner.

Recommendation – We recommend that AOC perform the following:

- Conduct a comprehensive risk assessment using NIST SP 800-30 methodology to identify risks and implement appropriate mitigating controls to address the vulnerabilities including those identified in SAS 70 audit reports
- Complete the implementation of the security plans
- Revise customer help desk incident response procedures to include responsibilities for security incident response
- Define IT division (ITD) positions, including level of sensitivity
- Require all AOC employees to receive annual security awareness training as well as require IT security staff to receive specialized training for assigned job duties and maintain evidence of such training
- Develop a formal process to address observations from security reviews, which should include independent evaluation of the corrective action
- Document user profiles and include them in the system security plans

- Develop and implement user account management procedures to ensure timely removal or modification of user accounts and assigned privileges
- Implement monitoring procedures in accordance with NIST SP 800-92, to ensure network management is compliant with ITD policies and procedures
- Implement network management tools and procedures to enhance control
- Continue to develop a comprehensive COOP/DRP, perform tests of the plans, and make necessary changes based on results.

2. Time Recordation, Processing, and Approval Procedures (Repeat Condition)

We identified the following instances in which AOC time recordation and payroll was not properly authorized:

- Out of a sample of seventy-eight, thirty employees were either missing an overtime approval form, did not have the required authorizing signature, or did not obtain approval before the overtime was taken
- Out of a sample of seventy-eight, twelve leave request forms were not approved prior to the leave being taken.

Recommendation – We recommend that AOC ensure that policies concerning the approval and entering of time are strictly enforced.

We also identified other, less significant matters that will be reported to AOC's management in a separate letter.

This report is intended solely for the information and use of the Office of Inspector General of AOC, AOC management, GAO, and the U.S. Congress, and is not intended to be, and should not be used by anyone other than these specified parties.

Kearney & Company

January 16, 2008
Alexandria, Virginia